PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

INTRODUCCIÓN

La Seguridad de la Información en las entidades tiene como objetivo la protección de los activos de información en cualquiera de sus estados ante una serie de amenazas que atenten contra sus principios fundamentales de confidencialidad, integridad y su disponibilidad, a través de la implementación de medidas de control de seguridad de la información, que permitan gestionar y reducir los riesgos e impactos a que está expuesta.

La Gobernación de Nariño enmarcada en el proceso anteriormente descrito y con el fin de dar cumplimiento a la política de seguridad de la información, debe aplicar el modelo de administración de los riesgos de seguridad de la información y las actividades de valoración de mismos riesgos, como medio o herramienta para el logro de los objetivos de mantener la información de la Entidad confidencial, íntegra y disponible, a través de su ciclo de vida desde su captura, almacenamiento, explotación, hasta su eliminación, para el correcto desempeño dentro de la política pública y su relación con el ciudadano

Los principios de protección de la información se enmarcan en:

• Confidencialidad: Propiedad que la información sea concedida únicamente a quien esté autorizado.

• Integridad: Propiedad que la información se mantenga exacta y completa.

• Disponibilidad: propiedad que la información sea accesible y utilizable en el momento que se requiera.

OBJETIVO GENERAL

Presentar el Plan de acción para la elaboración del Plan de Tratamiento para los riesgos de seguridad y privacidad de la información, identificados en los procesos incluidos en el alcance del Sistema de Seguridad de la Información y MIPG alineadas con la Norma NTC/IEC ISO 27001:2013, la Política de Seguridad Digital y Continuidad del servicio

El Plan de Tratamiento para los riesgos de seguridad y privacidad de la información permita disminuir la probabilidad y el impacto de riesgos de seguridad y privacidad de la información que puedan afectar a la Gobernación de Nariño. para proporcionar una seguridad e integridad razonable que genere una base confiable para la toma de decisiones y la planificación institucional.

OBJETIVOS ESPECÍFICOS

1. Identificar y sensibilizar a la entidad para la construcción de acciones que conlleven al fortalecimiento de la Entidad frente a la seguridad y privacidad de la información.

2. Revisar, ajustar y/o validar la Política de la Entidad de Gestión de Riesgos de seguridad y privacidad de la información.

3. Generar un panorama de la Entidad para la construcción de planes políticas y controles para un adecuado tratamiento de riesgo de seguridad y privacidad de la información.

4. Definir y desarrollar estrategias para la elaboración del plan de tratamiento de riesgos de seguridad y privacidad de la información con priorización de aspectos críticos identificados, validando los recursos con los que se cuentan actualmente en la Gobernación de Nariño.

5. Conocer y explorar las metodologías del DAPF[1] e ISO[2] respectivamente en seguridad y riesgo de la información.

ALCANCE

La gestión de riesgos de seguridad de la información y su tratamiento, deberá será aplicada sobre cualquier proceso de la Gobernación de Nariño, a cualquier sistema de información o aspecto particular de control de la Entidad, a través de los principios básicos y metodológicos

[1] DAPF es el Departamento Administrativo de la Función Pública de Colombia ISO

[2] ISO es International Organization for Standardization, que en español traduce, Organización Internacional de Normalización

para la administración de los riesgos de seguridad de la información, así como las técnicas, actividades y formularios que permitan y faciliten el desarrollo de las etapas de reconocimiento del contexto, identificación de los riesgos de seguridad de la información, análisis y evaluación, opciones de tratamiento o manejo del riesgo según la zona de riesgo; incluye además pautas y recomendaciones para su seguimiento, monitoreo y evaluación.

NORMATIVIDAD

La normatividad en el cual se enmarca el Plan Tratamiento de Riesgos de Seguridad y Privacidad de la Información, se encuentra dentro del marco de la legislación alusiva al Sistema de gestión pública del Estado Colombiano, especialmente de la Política de Gobierno Digital y articulada con la reglamentación y lineamientos producidos por la legislación Colombiana, Decreto reglamentarios, el Departamento Administrativo de la Función Pública y el Ministerio de las TIC, como, Habeas DATA, Propiedad Intelectual, Seguridad Digital, Servicios Ciudadanos Digitales, Participación Democrática, Transparencia, Acceso a la Información Pública y Anticorrupción, entre otros.

RESPONSABILIDAD Y AUTORIDAD El desarrollo y actualización del plan está bajo la autoridad de la Dirección o área responsable del proceso de Gestión Tecnológica, o quién haga sus veces dentro del contexto de las Tecnologías de la Información y las Comunicaciones que establezca oficialmente la Gobernación de Nariño para tal finalidad, o quién lo reemplace o sustituya. Actualmente es la Secretaria TIC, Innovación y Gobierno Abierto, quien podrá editar el contenido de cada una de las secciones que lo conforman, previa aplicación del comité MIPG.

PLAN DE ACCIÓN

1. DIAGNÓSTICO DE LA SITUACIÓN ACTUAL: OBTENER UNA VISIÓN GENERAL DEL PROCESO DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

A. Involucrar a los participantes e interesados, para ello es necesario consolidar el grupo encargado de construir el Plan de tratamiento de Riesgos de Seguridad Informático y contar con el compromiso de la Alta Dirección

B. Con el fin de determinar y Gestionar los riesgos de seguridad y privacidad de la información de manera integral, y así realizar el plan de tratamiento de riesgos, es necesario conocer el estado de implementación de la política general de seguridad y privacidad de la información.

C. Analizar el entorno y la normatividad vigente: Realizar un análisis de los factores externos políticos, económicos, sociales, tecnológicos y normatividad vigente que afecta la entidad pública.

2. ESTABLECIMIENTO DEL CONTEXTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

A. Identificar los riesgos de seguridad informática asociados a los procesos que hacen parte del alcance del SGSI

En esta etapa es necesario definir la metodología e instrumentos para la revisión de la Guía y Herramienta de Gestión de Riesgos de Seguridad y privacidad de la Información, Seguridad Digital y Continuidad de la Operación, establecidos en la política general de seguridad y privacidad de la información.

B. Consolidar la matriz de riesgos de Seguridad Informática

Con la Matriz de riesgos – SIMIG establecida, es necesario identificar las fuentes que pueden dar origen a los riesgos y oportunidades en los procesos de la Entidad, así como el análisis de las debilidades y amenazas asociadas, en la valoración de los riesgos y las consecuencias para la Entidad y en la probabilidad de su ocurrencia

C. Establecer los siguientes aspectos:

a. Criterios de evaluación del riesgo de seguridad de la información, enfocados en la criticidad de los activos de información involucrados, requisitos legales y reglamentarios, importancia de la disponibilidad, integridad y confidencialidad para los procesos de Entidad

b. Criterios de Impacto, especificados en términos de grado, daño o costo para la Entidad, tales como: clasificación de los activos de la información, incumplimiento de las fechas límites o planes, incumplimiento de requisitos legales

c. Criterios de Aceptación, dependen de las metas de la Entidad, por lo cual es necesario definir las escalas de aceptación de riesgos de seguridad de la información

3. VALORACIÓN DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Durante esta etapa se tiene en cuenta los activos de la información identificados, ya que son la base para la valoración de los riesgos de seguridad de la información. Se deberán identificar los riesgos, describir cuantitativamente o cualitativamente y priorizar frente a los criterios de evaluación determinados en la fase anterior

La valoración del Riesgo de seguridad de la información consta de las siguientes actividades:

A. Identificación del riesgo. Se deberán identificar los activos de información por proceso, teniendo en cuenta su clasificación

Primarios:

Procesos o subprocesos y actividades del Negocio: procesos cuya modificación y/o pérdida hacen imposible o afectar de manera muy significativa la misión de la Entidad, procesos que son necesarios para el cumplimiento de los requisitos contractuales, legales o reglamentarios.

Información: información vital para la ejecución de la misión de la Entidad, información estratégica que se requiere para alcanzar los objetivos estratégicos de la Entidad, información de alto costo cuya recolección, almacenamiento, procesamiento y transmisión exigen un largo periodo de tiempo y/o implican un alto costo de adquisición.

Actividades y procesos de negocio: que tienen que ver con propiedad intelectual, los que si se degradan hacen imposible la ejecución de las tareas de la empresa, los necesarios para el cumplimiento legal o contractual, etc.

De Soporte

Hardware: Elementos físicos que dan soporte a los procesos (PC, portátiles, servidores, impresoras, discos, documentos en papel, etc.).

Software: Programas que contribuyen al funcionamiento de la Entidad (sistemas operativos, paquetes de software o estándar, aplicaciones, mantenimiento o administración, etc.)

Redes: Dispositivos de telecomunicaciones tales como conmutadores, cableado, puntos de acceso, etc.

Personal: Grupos de personas involucradas en el sistema de información (usuarios, desarrolladores, responsables, etc.)

Sitio: Lugares en los cuales se pueden aplicar los medios de seguridad de la organización (Edificios, salas, y sus servicios, etc.)

Estructura organizativa: responsables, áreas, contratistas, etc.

Una vez clasificados los activos de la información se deben determinar los mecanismos a utilizar para identificar y valorar las **amenazas** que pueden causar daños en la información, los procesos y los soportes, así mismo los cronogramas de aplicación. Una vez identificadas las amenazas se identifican las vulnerabilidades y las consecuencias es decir cómo se afecta la confidencialidad, integridad y disponibilidad de los activos de información

B. Estimación del riesgo

La estimación del riesgo busca establecer la probabilidad de ocurrencia de los riesgos y el impacto de sus consecuencias, calificándolos y evaluándose con el fin de obtener información para establecer el nivel de riesgo, su priorización y estrategia de tratamiento de estos. El objetivo de esta etapa es el de establecer una valoración y priorización de los riesgos.

Para la estimación es necesario contar con el personal que tenga conocimiento de los procesos ya que se debe tener en cuenta pérdidas financieras, costos de reparación o sustitución, interrupción del servicio, infracciones legales, competitiva, daños personales, entre otros.

Además de medir las posibles consecuencias se deberán definir los mecanismos para estimar la probabilidad de ocurrencia de situaciones que generen impactos sobre los activos de información, se deberán calificar el impacto y la probabilidad de cada uno de los riesgos identificados de acuerdo con los niveles para la estimación de los riesgos.

C. Evaluación del riesgo

Una vez se valoran los impactos, la probabilidad y las consecuencias de los escenarios de incidentes sobre los activos de información, se obtendrán los niveles de riesgo, con ello es necesario definir los mecanismos de evaluación que permitirán compararlos frente a los criterios básicos del contexto, con el fin de tomar decisiones adecuadas basados en reducir los impactos en riesgos de seguridad de la información.

4. TRATAMIENTO DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

En esta etapa se deberá elegir los mecanismos y/o estrategia de tratamiento del riesgo según su valoración y de los criterios establecidos en el contexto de gestión de riesgos, según la matriz de riesgos que contiene la identificación de los niveles de riesgo de acuerdo con la zona de ubicación, obtenida en las etapas anteriores.

Se deberá seleccionar la opción de tratamiento por cada uno de los riesgos identificados, de acuerdo con el nivel evaluación de los riesgos, así como tener en cuenta como factor relevante el costo/beneficio del tratamiento para la decisión.

COSTO - BENEFICIO	OPCIÓN DE TRATAMIENTO
El nivel de riesgo está muy alejado del nivel de tolerancia, su costo y tiempo del tratamiento es muy superior a los beneficios	**Evitar** el riesgo, su propósito es no proceder con la actividad o la acción que da origen al riesgo (ejemplo, dejando de realizar una actividad, tomar otra alternativa, etc.)
El costo del tratamiento por parte de terceros (internos o externos) es más beneficioso que el tratamiento directo	**Transferir o compartir** el riesgo, entregando la gestión del riesgo a un tercero (ejemplo, contratando un seguro o subcontratando el servicio).
El costo y el tiempo del tratamiento es adecuado a los beneficios	**Reducir o Mitigar** el riesgo, seleccionando e implementando los controles o medidas adecuadas que logren que se reduzca la probabilidad o el impacto
La implementación de medidas de control adicionales no generará valor agregado para reducir niveles de ocurrencia o de impacto.	**Retener o aceptar** el riesgo, no se tomará la decisión de implementar medidas de control adicionales. Monitorizarlo para confirmar que no se incrementa

Como resultado de esta fase se seleccionan las opciones de tratamiento para cada riesgo identificado, que permitan establecer la relación de riesgos residuales, es decir, aquellos que aún siguen existiendo a pesar de las medidas tomadas, lo anterior deriva en el plan de tratamiento de riesgos, en el cual se identifican los controles aplicables considerando las posibles limitantes para su implementación tales como restricciones de tiempo, financieras, técnicas, operativas, culturales, éticas, ambientales, legales, uso, de personal, entre otros

5. MONITOREO Y SEGUIMIENTO DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Teniendo en cuenta que los riesgos son dinámicos y pueden cambiar de forma sin ser previsto es necesario definir mecanismos que permitan hacer una supervisión continua que detecte: nuevos activos o modificaciones en el valor de los activos, nuevas amenazas, cambios o aparición de nuevas vulnerabilidades, aumento de las consecuencias o impactos, incidentes de seguridad de la información.

En este sentido se deben establecer instrumentos para realizar la revisión del valor de los activos, impactos, amenazas, vulnerabilidades y probabilidades en busca de posibles cambios, que exijan la valoración iterativa de los riesgos de seguridad de la información.

También se deberán definir esquemas de seguimiento y medición al sistema de gestión de riesgos de la seguridad de la información, con el propósito de conocer los estados de cumplimiento de los objetivos de la gestión de los riesgos de seguridad de la información